



DIRENZIC
Technology Consulting Group

CYBERSECURITY & AI GOVERNANCE

FOR CRITICAL SYSTEMS

Building Safer Systems for a Better Tomorrow

ICS/SCADA Cybersecurity Assessments

Penetration Testing: Cyber and Physical

NIST 800-53 and CMMC Compliance Readiness

vCISO (Virtual Chief Information Security Officer) Services

Direnzi Technology Consulting Group, LLC delivers executive-level cybersecurity leadership, AI governance, and critical infrastructure protection to federal agencies, state and municipal governments, and private sector partners. We specialize in water utilities, transit systems, industrial control environments, and OT/IT convergence, translating complex cyber and AI threats into clear, actionable strategies for executives and operational teams. As a certified Woman- and Minority-Owned small business, we embed experienced security leadership through vCISO services, AI governance programs, and strategic advisory.

DESIGNATIONS

100% Woman and Minority Owned

WOSB / EDWOSB | MBE | WBE
DBE (LA, TN, GA)
Hudson Initiative | Fair Share
Pursuing: SBA 8(a) and GSA
Schedule

CORE CAPABILITIES

ICS / SCADA Security

OT cyber risk analysis, SCADA
architecture review, ICS assessments

Critical Infrastructure Risk

Water, transit, manufacturing and
municipal resilience

NIST / CMMC / SOC 2 Compliance

Risk management, audit readiness,
ISO 27001 preparation

Penetration Testing

Cyber and physical pen testing,
vulnerability and insider threat
analysis

vCISO Services

White-label delivery, board advisory,
enterprise risk management

AI Governance

AI Risk and Readiness Assessment,
ARG-CRP, defensibility posture

Incident Response and Training

IR planning, tabletop exercises,
workforce development

NAICS AND PSC CODES

Primary: 541519

Other Computer Related Services
541611 Admin and General Mgmt
Consulting
541690 Technical Consulting
Services
611420 Computer Training
611430 Professional Development
Training
561320 Temporary Help Services

PSC Codes: D310 | U012

PROFESSIONAL CERTIFICATIONS

PMP | CISSP | CISA | CEH |
GXPN
Six Sigma | NIST and CMMC

Compliance

SAM Registered

WHY AGENCIES AND PARTNERS CHOOSE DIRENZIC

Critical Infrastructure Specialists

Deep expertise securing water utilities, transit, and municipal OT/IT environments. Not a generalist firm.

Proven Government Performance

Supporting organizations aligned with EPA, DHS, CISA and FBI programs across multiple states.

AI Governance Defensibility Authority

Proprietary AIRisk and Readiness Assessment and ARG-CRP program position Direnzi as the AI governance defensibility leader for critical infrastructure.

Cyber and Physical Security Integration

Unique capability to assess both digital systems and physical operational infrastructure in a single engagement.

White-Label vCISO Ready

Co-branded or white-label vCISO delivery for MSPs, cybersecurity firms, and teaming partners.

Educational, Non-Technical Approach

We translate risk into language executives and operators understand, driving buy-in and measurable action.

REPRESENTATIVE PAST PERFORMANCE

Workforce Solutions Greater Dallas

Multi-year cyber and physical penetration testing and immersive security awareness training across regional operations.

40% reduction in threat exposure

QNET IS, Inc.

vCISO and Compliance Readiness as a Service. Governance frameworks and streamlined compliance across client portfolios.

100% regulatory compliance achieved

Monroe City Transit Authority

SMART transit technology across LA, TX, CA and FL. Real-time passenger tracking and safety infrastructure deployment.

20% system reliability improvement

Monroe Water Treatment Plant

\$42M infrastructure subcontract. SCADA security config, fiber network design, and cybersecurity integration with city engineers.

25% project efficiency increase

Shreveport AMISS Water Project

CISO consultant and vulnerability management lead for municipal water systems. Insider threat mitigation. \$2M subcontract.

50% cybersecurity risk reduction

Tensas Community Health Center

Digital forensic investigations supporting civil litigation. Full chain-of-custody integrity maintained throughout.

Healthcare sector forensic support

TARGET AGENCY PARTNERS

Dept. of Homeland Security (DHS)
Cybersecurity and Infrastructure Security Agency (CISA)
Environmental Protection Agency (EPA)
Dept. of Transportation (DOT)
State and Municipal Water and Wastewater Utilities
Transit Authorities and Transportation Agencies

CONTRACTING INFORMATION

Entity: Direnzi Technology Consulting Group, LLC

UEI: JJGDZES9AQB3

CAGE Code: 6TDG7

Primary NAICS: 541519

PSC Codes: D310 | U012

SAM.gov: Registered

Socioeconomic: WOSB EDWOSB MBE WBE DBE

Pursuing: SBA 8(a) and GSA Schedule

www.direnzi.com
contact@direnzi.com
(214) 995-2642

500+

leshea Hollins, Your Cybersecurity + AI Governance C-Suite Partner

Founder and CEO | vCISO
Chief Cybersecurity and AI Strategist



CYBERSECURITY & AI GOVERNANCE FOR CRITICAL INFRASTRUCTURE

Building Safer Systems for a Better Tomorrow

AI GOVERNANCE DEFENSIBILITY

Direnzic occupies a distinct position at the intersection of cybersecurity and artificial intelligence governance. As AI adoption accelerates across critical infrastructure, government contractors, and regulated industries, the critical question is whether an organization's AI usage is defensible. Direnzic is the AI Governance Defensibility Authority, offering proprietary programs including the AI Risk and Readiness Assessment (Executive Edition) and the AI Risk Governance and Cyber Resilience Program (ARG-CRP) that move organizations from reactive AI adoption to a documented, auditable, and defensible governance posture. Available as standalone engagements and as partner-delivered solutions for MSPs and teaming partners.

RESULTS AT A GLANCE

45%
improvement in compliance readiness
30 to 45%
reduction in cyber risk exposure within 6 months
30%
faster incident response post tabletop exercises
120 Days
average SOC 2 readiness timeline

MARKETS SERVED

Critical Infrastructure
Water and Wastewater Utilities
Transportation and Transit
Healthcare
Manufacturing
Government Agencies
Entertainment
Education

WHY AGENCIES AND PARTNERS CHOOSE DIRENZIC — AN EXPANDED VIEW

20+ Years Critical Infrastructure Experience

Two decades of hands-on cybersecurity, digital forensics, and infrastructure risk management across water, transit, and government sectors.

Embedded Security Leadership

We place experienced vCISO-level leadership inside your organization, bridging strategy, governance, and execution.

OT and IT Security Convergence

Direnzic bridges IT and OT environments, securing the full operational environment from industrial control systems to enterprise networks.

Measurable, Documented Outcomes

Every engagement is scoped to produce quantifiable results. Clients see reduced risk exposure, improved compliance scores, and faster incident response.

Multi-Framework Compliance Expertise

NIST CSF, NIST 800-53, CMMC, SOC 2, and ISO 27001 expertise in a single team. No need to hire multiple specialists.

Small Business Agility with Enterprise Depth

Certified small business with the credentials and experience to compete on federal and state contracts alongside large primes.

Trusted by Government-Adjacent Programs

Engagements supporting organizations aligned with EPA, DHS, CISA, and FBI programs demonstrate readiness to operate in rigorous government environments.

Teaming and Subcontracting Ready

Available as a prime, subcontractor, or teaming partner. White-label vCISO and AI governance delivery for MSPs expanding their service portfolio.

Proactive Risk Strategy

We prioritize early detection, governance maturity, and resilience planning so clients avoid costly incidents rather than recovering from them.

PAST PERFORMANCE — SCOPE, APPROACH AND OUTCOMES

Workforce Solutions Greater Dallas

Scope: Multi-year cybersecurity engagement including cyber and physical penetration testing and immersive security awareness training.
Approach: Conducted layered assessments targeting digital vulnerabilities and physical access control weaknesses, then designed tailored training to shift organizational security culture.
Outcome: 40% reduction in threat exposure and measurably stronger cybersecurity posture across regional operations.

QNET IS, Inc.

Scope: Ongoing third-party cybersecurity partner providing vCISOaaS and Compliance Readiness as a Service across a diverse client portfolio.
Approach: Implemented governance frameworks, streamlined compliance across multiple regulatory environments, and provided board-level cybersecurity advisory.
Outcome: 100% regulatory compliance achieved across all client accounts.

Monroe Water Treatment Plant

Scope: Subcontractor under Max Foote Construction Co. on a \$42M municipal water treatment infrastructure project.
Approach: Led secure SCADA system configuration, fiber network architecture design, and cybersecurity integration in direct collaboration with city engineers.
Outcome: 25% increase in project efficiency. Seamless cybersecurity and operational continuity achieved throughout.

Monroe City Transit Authority

Scope: SMART technology implementation across transit systems in Louisiana, Texas, California, and Florida.
Approach: Deployed real-time passenger tracking, integrated safety infrastructure, and secured technology environments across all transit locations.
Outcome: 20% improvement in system reliability and passenger satisfaction across all markets.

Shreveport AMISS Water Project

Scope: vCISO consultant and vulnerability management lead for municipal water systems under a \$2M subcontract.
Approach: Directed insider threat mitigation, interactive staff training, vulnerability remediation, and full project management oversight.
Outcome: 50% reduction in cybersecurity risk exposure for municipal water systems.

Tensas Community Health Center

Scope: Digital forensic investigation and data retrieval supporting civil litigation for a rural healthcare organization.
Approach: Performed structured forensic data retrieval, maintained chain-of-custody documentation, and delivered court-ready evidence packages.
Outcome: Case success achieved. Critical forensic evidence delivered with full chain-of-custody integrity maintained.